IN THE CLAIMS:

Please amend claims 9, 10, 17, and 23-36;

cancel claims 11-13; and

add new claims 37-39 as follows.

1. (Previously Presented) A method, comprising:

extracting a routing information from a received message at a border between a first network and a second network;

adding at least one invalid entry to first-network entries of said routing information to blur or hide an actual number of routing entries which correspond to routing nodes through which said received message has been routed, said first-network entries relating to a routing path of said message within said first network;

generating an encrypted routing information by encrypting said at least one invalid entry and said first-network entries by using an own token at least for each of said first-network entries;

replacing said routing information of said received message by said encrypted routing information; and

forwarding said received message with said encrypted routing information to said second network.

2. (Previously Presented) The method according to claim 1, further comprising providing said routing information in a routing header of said message.

3. (Currently Amended) The method according to claim 2, further comprising providing said routing header comprising a record-route header of a session initiation protocol message and a service-route header as specified for the ~~ession~~ session initiation protocol.

4. (Previously Presented) The method according to claim 1, further comprising processing said routing information using a topology hiding method.

5. (Previously Presented) The method according to claim 4, wherein, in said processing, said topology hiding method is applied in response to a user identity marked with a predetermined information.

6. (Previously Presented) The method according to claim 4, wherein, in said processing, said topology hiding method is applied in response to a network identity.

7. (Previously Presented) The method according to claim 1, further comprising marking said at least one added invalid entry.

8. (Previously Presented) The method according to claim 1, further comprising providing each of said first-network entries comprising at least one of name

and address information of a network node through which said received message has been routed.

9. (Currently Amended) The method according to claim 1, further comprising providing said border between said first and second networks, wherein said border is defined at a gateway ~~device~~ which said message traverses on a connection between said first and second networks.

10. (Currently Amended) ~~A device~~ An apparatus, comprising:

extracting means for extracting ~~said~~ routing information from a received message at a border between a first network and a second network;

adding means for adding at least one invalid entry to first-network entries of said routing information to blurr or hide an actual number of routing entries which correspond to routing nodes through which said received message has been routed, said first-network entries relating to a routing path of said message within said first network;

encrypting means for generating an encrypted routing information by encrypting said at least one invalid entry and said first-network entries by using an own token at least for each of said first-network entries;

replacing means for replacing said routing information of said received message by said encrypted routing information; and

forwarding means for forwarding said received message with said encrypted routing information to said second network.

11-13. (Cancelled)

14. (Previously Presented) A method, comprising:

extracting a routing information from a received message at a border between a first network and a second network;

generating a decrypted and reversed routing information by decrypting a tokenized second-network entry relating to a routing path of said message within said second network and by reversing the content of the decrypted second-network entry;

replacing said routing information of said received message by said decrypted and reversed routing information; and

forwarding said received message with said decrypted and reversed routing information to said second network.

15. (Previously Presented) The method according to claim 14, further comprising:

conveying said routing information in a routing header of said message.

16. (Previously Presented) The method according to claim 15, wherein said routing header comprises at least one of a route header and a via header of a session initiation protocol message.

17. (Currently Amended) The method according to ~~any~~ claim 14, further comprising:

using a topology hiding method.

18. (Previously Presented) The method according to claim 17, further comprising applying said topology hiding method in response to a user identity marked with a predetermined information.

19. (Previously Presented) The method according to claim 17, further comprising

applying said topology hiding method in response to a network identity.

20. (Previously Presented) The method according to claim 14, wherein said tokenized second-network entry comprises at least one of an encrypted name and encrypted address information of a sequence of network nodes through which said received message has been routed.

21. (Previously Presented) The method according to claim 14, further comprising:

marking a tokenized network entry of at least one of an incoming and an outgoing tokenizing network node; and

suppressing said reversing at outgoing tokenizing network nodes.

22. (Previously Presented) The method according to claim 14, further comprising:

marking a tokenized network entry of at least one of an incoming and an outgoing tokenizing network node; and

reversing network entries at incoming tokenizing network nodes before encryption.

23. (Currently Amended) The method according to claim 14, wherein said border between said first and second networks is defined at a gateway ~~device~~ which said message traverses on a connection between said first and second networks.

24. (Currently Amended) ~~A device~~ An apparatus, comprising:

extracting means for extracting a routing information from a received message at a border between a first network and a second network;

decrypting and reversing means for generating a decrypted and reversed routing information by decrypting a tokenized second-network entry relating to a routing path of said message within said second network and by reversing the content of the decrypted second-network entry;

replacing means for replacing said routing information of said received message by said decrypted and reversed routing information; and

forwarding means for forwarding said received message with said decrypted and reversed routing information to said second network.

25. (Currently Amended) The ~~device~~ apparatus according to claim 24, further comprising one of an interrogating call ~~Session~~ session control function and a topology hiding gateway function.

26. (Currently Amended) The ~~device~~ apparatus according to claim 24, wherein said apparatus operates in a packet data network which comprises an Internet protocol ~~(IP)~~ multimedia subsystem.

27. (Currently Amended) The ~~device~~ apparatus according to claim 24, wherein said ~~network device~~ apparatus is configured to suppress reversing of said decryptor and reverser when said routing information indicates that said ~~network device~~ apparatus is an outgoing tokenizing network node.

28. (Currently Amended) The ~~device~~ apparatus according to claim 24, wherein said ~~network device~~ apparatus is configured to reverse network entries before encryption when said routing information indicates that said ~~network device~~ apparatus is an incoming tokenizing ~~network node~~ apparatus.

29. (Currently Amended) The ~~device~~ apparatus according to claim 24, wherein said border between said first and second networks is defined at said ~~network device~~ apparatus.

30. (Currently Amended) ~~A device~~An apparatus, comprising:

an extractor configured to extract a routing information from a received message at a border between a first network and a second network;

an adder, operably connected to said extractor, and configured to add at least one invalid entry to first-network entries of said routing information to blurr or hide an actual number of routing entries which correspond to routing nodes through which said received message has been routed, said first-network entries relating to a routing path of said message within said first network;

an encryptor, operably connected to said extractor, and configured to generate encrypted routing information by encrypting said at least one invalid entry and said first-network entries by using an own token at least for each of said first-network entries;

a replacer, operably connected to said extractor, and configured to replace said routing information of said received message by said encrypted routing information; and

a transmitter, operably connected to said extractor, and configured to forward said received message with said encrypted routing information to said second network.

31. (Currently Amended) ~~A device~~ An apparatus, comprising:

an extractor configured to extract a routing information from a received message at a border between a first network and a second network;

a decryptor, operably connected to said extractor, and configured to generate a decrypted and reversed routing information by decrypting a tokenized second-network entry relating to a routing path of said message within said second network and further configured to reverse the content of the decrypted second-network entry;

a replacer, operably connected to said extractor, and configured to replace said routing information of said received message by said decrypted and reversed routing information; and

a transmitter, operably connected to said extractor, and configured to forward said received message with said decrypted and reversed routing information to said second network.

32. (Currently Amended) The ~~device~~ apparatus according to claim 31, further comprising:

one of an interrogating call session control function and a topology hiding gateway function.

33. (Currently Amended) The ~~device~~ apparatus according to claim 31, wherein said apparatus operates in a packet data network which comprises an Internet protocol ~~(IP)~~ multimedia subsystem.

34. (Currently Amended) The ~~device~~ apparatus according to claim 31, wherein said ~~device~~ apparatus is configured to suppress reversing of said decrypter when said routing information indicates that said ~~network device~~ apparatus is an outgoing tokenizing ~~network node~~ apparatus.

35. (Currently Amended) The ~~device~~ apparatus according to claim 31, wherein said ~~device~~ apparatus is configured to reverse network entries before encryption when said routing information indicates that said ~~device~~ apparatus is an incoming tokenizing ~~network node~~ apparatus.

36. (Currently Amended) The ~~network device~~ according to claim 31, wherein said border between said first and second networks is defined at said ~~device~~ apparatus.

37. (New) The apparatus according to claim 30, wherein said apparatus further comprises one of an interrogating call session control function and a topology hiding gateway function.

38. (New) The apparatus according to claim 30, wherein said apparatus operates in a packet data network which comprises an Internet protocol multimedia subsystem.

39. (New) The apparatus according to claim 30, wherein said border between said first and second networks is defined at said apparatus.